電子化知的財産・社会基盤　6－6
（1999. 10. 9）

金融システムにおけるバイオメトリックス認証

中山　靖司[†]　　小松　尚久[††]

[†]東京大学先端経済工学研究センター
〒153-8904　東京都目黒区駒場 4-6-1
nakayama@aee.u-tokyo.ac.jp

[††]早稲田大学理工学部 電子・情報通信学科
〒169-8555　東京都新宿区大久保 3-4-1
komatsu@kom.comm.waseda.ac.jp

あらまし　近年、情報技術の進展によって、金融サービスのほとんどはネットワークによって結ばれたコンピュータシステムによって実現されるようになってきており、一般の利用者がインターネット等を通じて自宅のパソコンからサービスを受けることも可能になってきている。ネットワークを介してサービスを提供する場合には、サービスを受けようとしている相手の真正性を確認することが重要であり、確実に本人を確認する手段としてバイオメトリックス認証が注目されている。本稿では、金融システムにおける本人認証の手段としてのバイオメトリックス認証の適用について、実用化や標準化の動向とともにその課題についてまとめる。

キーワード　バイオメトリックス、本人認証、本人照合、個人識別、標準化、金融サービス

Biometrics authentication in case of financial services

Yasushi NAKAYAMA[†]　　Naohisa KOMATSU[††]

[†]Research Center for Advanced Economic Engineering,
The University of Tokyo
4-6-1 Komaba, Meguro-ku, Tokyo 153-8904, Japan
nakayama@aee.u-tokyo.ac.jp

[††]School of Science and Engineering Department of Electronics,
Information and Communication Engineering,
WASEDA UNIVERSITY
3-4-1 Ohkubo Shinjuku-ku, Tokyo 169-8555, Japan
komatsu@kom.comm.waseda.ac.jp

Abstract　In recent years, with the developing of the information technology, the computer system which was linked by the network gets to realize most of the finance service and the general user becomes able to receive service from the personal computer at his house through the Internet and so on, too. When providing service through the network, to confirm the authenticity of the person who tries to receive service is important and the biometrics authentication is remarkable as the means of confirming the very person surely. This paper gathers about the problem with the trend of the coming to practical use and the standardization about the application of the biometrics authentication as the means of the very person authentication about the financial system.

key words　Biometrics, authentication, verification, identification, standardization, financial service

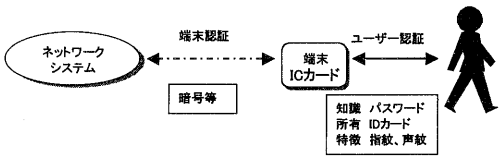
1. 金融サービスと個人認証の関わり

近年、情報技術の進展によって、現金の受払、振込／振替、残高確認等はもちろん金融サービスのほとんどはネットワークによって結ばれたコンピュータシステムによって実現されるようになってきている。このように、ネットワークを介してサービスを提供する時に重要なことは、サービスを受けようとしている相手の真正性を確認することである。ここでいう真正性とは、サービスを受けるために予め契約を結んでいる本人に間違いないということである。キャッシュカードやデビットカードでは、取引を行おうとしている相手がカードを保持し、かつ予め登録してある4桁の暗証番号を知っているということをATM等の機械によって確認することによって、本人であると判断している他、クレジットカードではカードを保持し、目の前でカードに予め記入されているのと同じ署名を行うことができることを商店が確認することによって行われることが普通である。

しかしながら、これらは安全性の面から必ずしも確実な手段とはいえず、多くの課題を抱えている。

2. 個人を認証する方法 [1]

(1) 端末＋ネットワークにおける本人認証



(図1)ネットワークにおいて端末を利用する場合の個人認証

一般にネットワークで端末を利用する場合の個人認証は図1に示すとおり、①ユーザと端末(あるいはネットワーク)間(以下、ユーザ認証)、②ネットワークと端末間(以下、端末認証)の2段階に分けられる。例えば、CA(Certification Authority)による電子認証の仕組みは、使用している端末の確認であり、必ずしもユーザの確認を行っているわけではない。

ユーザ認証の方法は、①本人所有によるもの、②本人知識によるもの、③本人固有の特徴によるもの、の大きく3つに分類することができる。「本人所有によるもの」は、鍵やIDカード等正当な本人しか持ち得ないはずの物を所有していることにより認証する方法である。鍵やIDカードが盗まれたり、複製が作られたりすると、第3者による成りすましを行うことが可能であるほか、本人が紛失する危険性もある。「本人知識によるもの」は、暗証番号やパスワード等正当な本人しか知らないはずの情報を示すことにより認証する方法であり、コンピュータシステムのアクセスコントロール等で使われている。ただし、他人が容易に想像できるようなパスワードを使用したり、うっかり他人に漏れたりすることによって、第3者に容易に成りすまされる危険性があるほか、本人が忘れてしまう危険性もある。「本人固有の特長によるもの」は、指紋や声紋、筆跡等を計測し、正当な本人固有の特徴と合致するかどうかを確認することによって認証する方法で、本人固有の情報をどう捉えるかが成りすましに対する耐性に影響する。

これらの様々な認証の方法は、システムで要求されるセキュリティのレベル、システムの処理量およびユーザの許容度を考慮して、利用するパラメータの種類や形態を考えることが必要である。

(2) 本人固有の特徴を用いたユーザ認証

本人所有および本人知識といった従来のパラメータの代替あるいは補完するものとして本人固有の特徴がある。これは、身体的特徴(physiological characteristics)と身体的特性(behavioral characteristics)の2つに分類できる。身体的特徴の代表例としては指紋、網膜あるいは顔等が挙げられ、身体的特性の代表例としては筆跡、音声が挙げられる(表1)。

(表1) ユーザ認証の方法とパラメータ

知識	所有	個人の特徴	
		身体的特徴	身体的特性
暗証番号、パスワード	IDカード、鍵	顔、掌形、網膜、虹彩、指紋	筆跡、声紋、キーストローク
忘却危険性	遺失可能性	身体障害等により特徴が変わる可能性	
登録データ ⇔ 入力データ		登録時の入力データ　入力データ ↓　↓ 個人の特性 ⇔ 個人の特性	

身体的特徴を利用した認証も身体的特性を利用した認証も、予め登録した情報と入力した情報が等しいという結果をもって本人であることを確認する点が共通している。これは、本人所有および本人知識によるユーザ認証にも当てはまる特徴である。さらに、筆跡、音声等の身体的特性には、何を書いても、あるいは何を言っても本人が特定できるという特徴が加わる。普段我々は、家族あるいは友人の筆跡あるいは声だけで、誰であるかが分かる場合が多い。すなわち、我々は無意識のうちに筆跡、音声から個人が特定できるパラメータを抽出し、その結果を利用して本人を特定しているのであろうと考えられる。このように、身体的特性を利用したユーザ認証は、予め登録したテキストの内容にとらわれることのない柔軟性に富むマン・マシン・インタフェースが実現できる可能性がある。なお、この身体的特性の分類を拡張したものとして、本人の行動様式をパラメータとして認証を行う考え方も提案されており[2]、更なる技術と適用の拡大が期待できる。

(3) バイオメトリックス認証の分類

(a) 照合(verification)と識別(identification)

「照合」(verification)とは、指紋あるいは音声などのパラメータの種類には拠らず、入力された本人の特徴を示す情報と、ユーザのIDに対応したシステム内の登録情報との1対1の対応関係を確認することである。両者の情報の差が予め設定した閾値以下であれば本人であると特定する。ユーザは認証時に、自分のIDを

システムに入力する必要がある。一方、システムに入力された本人の特徴を示す情報と、予めシステムの中に登録された情報を比較し、予め設定した閾値以下の最も近いものを探す方法が「識別」(identification)である。ユーザは認証時に、自分の ID をシステムに入力する必要はない。

(b) テキスト依存、テキスト独立とテキスト提示

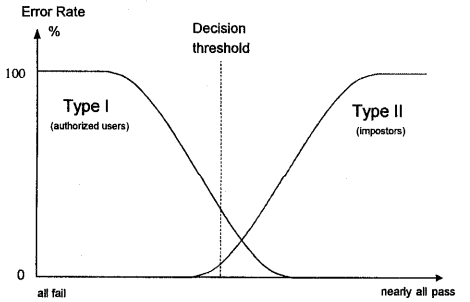
この分類は、身体的特性である音声あるいは筆跡を使った認証において使われるものである。「テキスト依存」とは、音声を例にすると、登録されたテキスト（音声の内容）と入力されたテキストが一致していることによって本人を特定する技術である。例えば署名照合は、典型的なテキスト依存型の個人認証方式である。これに対して「テキスト独立型」は、テキストの内容に依存せず、何を話しても、あるいは何を書いても本人であることを特定することが可能な技術である。また、「テキスト提示型」はチャレンジ／レスポンス型の個人認証方式である。前述のテキスト独立型の個人認証方式では、音声を録音すること等により第3者が特定の人物に成りすます危険性があるが、テキスト提示型の個人認証方式では、こうした成りすましを困難にするとともに、本人の特徴が現れ易いテキストをシステムが選択して提示することにより、信頼性の高い個人認証が実現できる可能性がある。

(c) オフライン情報の利用とオンライン情報の利用

筆跡を用いた個人認証の場合、予め紙等に書かれた筆跡をもとに認証を行うやり方が「オフライン型」であり、タブレットから筆跡情報をリアルタイムに入力して認証を行うものが「オンライン型」である。オンライン型の情報はオフライン型の情報に比べて種類が多く、また、まったく同じ入力を再度行うことはできないといった特徴があるなど、より安全性を高めることが可能であるため、ネットワークシステムにおいてはオンライン型を使用することが適当と考えられる。

(4) 認証時における誤りのタイプ

本人の身体的な特徴あるいは特性を用いて本人を特定する場合、誤りの有無や程度をどう捉えるかは非常に重要なポイントの一つである。個人の特徴を用いたバイオメトリックス認証の場合は、通常、登録情報と入力情報の距離がゼロとなることはあり得ず、入力時の条件に応じて距離が発生する。したがって、どの程度入力された個人の特徴を示す情報と登録されている情報が似ているか、という観点から本人を特定せざるを得ず、統計的な取り扱いが必要となる。そこで問題となるのが、タイプⅠ、タイプⅡという 2 種類の誤りである。タイプⅠ(FRR: False Rejection Rate)の誤りとは、システムにアクセスしているのが本人であるにもかかわらずシステムがリジェクトする誤りである。一方、タイプⅡ(FAR: False Acceptance Rate)の誤りとは、他人に対して正しい本人であると判定してしまう誤りである。通常の場合では、本人の特徴と他人の特徴には多かれ少なかれ類似性があり、部分的にオーバーラップしていると考えられる。この場合、タイプⅠの誤りとタイプⅡの誤りがクロスするポイントが存在する。すなわち、ある閾値を決めるとタイプⅠの誤りとともにタイプⅡの誤りが同時に発生することになる（図 2）。タイプⅡの誤りは他人をアクセプトしてしまう誤りであり、システムの安全性に関わる重大な誤りである。それに対し、タイプⅠの誤りは本人がリジェクトされてしまう誤りであり、システムの安全性というよりサービスに関わる誤りといえる。



（図2） 誤りのタイプと閾値の関係（一般的な場合）

一般的に安全性を重視するシステムであればある程、タイプⅡの誤りを小さく設定する必要がある。逆に、サービス性を重視すべきシステムでは、あまりタイプⅡの条件を厳しく設定すると本人が何度アクセスしてもリジェクトされてしまうことになりかねないため、まず、タイプⅠの誤りの程度を定め、このときのタイプⅡの誤りが安全性の設計の観点から許容できる値であることを確認するといったアプローチが考えられる。なお、タイプⅡの誤りは、暗証番号等の他の安全性を確保する手段の併用により、減少させることは可能であるが、タイプⅠの誤りは、他の手段を併用してもこれを減少させることは原理的に不可能であるため、多くのユーザがバイオメトリックス認証を利用するシステムでは、タイプⅡよりはむしろタイプⅠの誤りの低減を考慮すべきであると考えられる。

(表2) バイオメトリック認証の特徴

	パラメータ	特　徴	課　題
指紋	•特徴点（マニューシャ）の位置 •リレーション	•万人不同，終生不変 •犯罪捜査での利用	•指紋画像の品質 •衛生面の確保 •社会的な受容（プライバシー）
網膜	•毛細血管パターン	•万人不同，終生不変 •コピーが困難	•システムの規模，価格 •赤外線照射に対する抵抗感
虹彩	•瞳孔の開きを調節する筋肉のパターン	•万人不同，終生不変 •眼球内部の疾病等の影響がない	
掌形	•掌の幅，厚さ •指の長さ等	•操作が容易	•信頼性の確保 •衛生面の確保
顔	•目，口，鼻の位置や形状等	•非接触で認証可能 •心理的抵抗が少ない	•時間的な変化 •メガネ，ひげ等の影響 •照明や撮像角度，背景等の制約 •システムの規模，価格
音声	•スペクトル包絡 •ピッチ，発音レベル，発声速度等	•非接触で認証可能 •心理的抵抗が少ない •テキスト依存型	•テキスト独立，テキスト提示型の実用化 •時間的な変化 •体調の影響
筆跡	•筆順，筆速，筆圧等	•心理的抵抗が少ない •操作が容易（小型タブレット） •テキスト依存型	•テキスト独立，テキスト提示型の実用化 •時間的な変化 •偽筆対策

3. バイオメトリックス認証の研究と実用化事例

(1) バイオメトリックス認証の研究事例

現在、表2のとおり、様々なパラメータを使ったバイオメトリックス認証の研究が行われており、一部では実用化されつつある。

(2) 金融サービスにおけるバイオメトリックス実用化事例

バイオメトリックス認証の実用化例としては、企業等の内部の入退出管理システム向けが多くみられる。これは、システムを利用するユーザの数が比較的少なく、また、組織内部に閉じたシステムであるため、導入が容易であることが要因と考えられる。金融機関でも、様々なバイオメトリックス認証を使用した入退出管理を実験ないし検討中の金融機関も複数みられるようである。しかしながら、一般の顧客を対象とする金融サービスにおいて、バイオメトリックス認証を使用する例はまだ数えるほどしかない。これは、①登録するユーザの数が膨大になることから、照合はともかく識別については性能要求が厳しくなること、②一般の顧客を相手にするため、安全性はもちろん利便性にも十分配慮する必要があること、等から様子を窺う先が多いためと思われる。

(a) 日本国内における事例

・声紋を活用した音声による本人確認システムを採用した銀行のテレフォンバンキング[1]
・虹彩により本人確認を行う、消費者金融業者のATM[2]

(b) 海外における事例

・指紋スキャナーで本人確認を行う信用組合(米)のATM[3]
・虹彩により本人確認を行う貯蓄貸付組合(英)のATM[4]
・指のパターンで本人確認を行う銀行(コロンビア)のATM[5]
・指紋認証を使った銀行(米)のオンラインバンキング[6]
・顔認識を使った自動小切手清算機(米)[7]

4. バイオメトリックス認証の標準化動向

(1) バイオメトリックス認証の主要な標準化活動

バイオメトリックス認証の標準仕様として検討が進められている主要なものとしては、HA-API[8]、BAPI[9]、BioAPI[10]等がある[11]。各々推進主体が違い、標準化しようとしている適用領域も微妙に異なっているが、個々のバイオメトリックス方式の処理方法やアルゴリズム自体は標準化の対象外とされ、特定のベンダーやバイオメトリックス技術に依存しないアプリケーションインターフェースの仕様を標準化の対象としている点で共通している。なお、最近になって、これらを全て統一し、国内標準、国際標準に仕立てようとする動きが出てきている。

(a) HA-API (Human Authentication – Application Program Interface)

もともとNational Registry社が米国防総省の依頼により開発したAPI仕様であるが、後に世間に幅広く普及させることによって、バイオメトリックス技術の相互互換性を確保することを企図して一般に公開された。1997年8月にRev.1.0が作成されたあと、1998年4月にRev.2.0までが発表されている。

(b) BAPI (Biometric Application Programming Interface)

I/O Software社がバイオメトリックスのハードウェア、ソフトウェアベンダーに声をかけて組織したワーキンググループによって提案された。デバイス固有の機能の使用有無によって使い分けられる3つの機能的に異なるレベルから構成されているのが特徴である。1998年9月にVersion 1.3が出ている。

(c) BioAPI

1998年4月にCompaq等が推進主体となって組織されたBioAPIコンソーシアムで開発されたバイオメトリックス技術のための標準API仕様である。コンソーシアムには、HA-APIのNational Registry社、BAPIのI/O Software社、NSAやNIST情報技術研究所の政府関係者等、様々な分野の組織が参加している。プラットフォームやデバイスに依存しないマルチレベルAPIを実現する仕様として、1998年12月にBioAPIのドラフトがコンソーシアムメンバーに対して公表されている。

(2) 標準仕様統一化の流れ

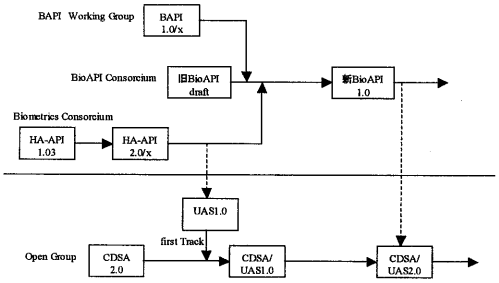
1998年12月、BAPIの設立主体であるI/O Software社がBioAPIの推進主体の一員として加わることになり、BAPIはVersion 1の完成を持って作業を終了し、その仕様はBioAPIに引き継がれることになった。さらに、1999年3月、BioAPIコンソーシアムとHA-APIのワーキンググループとの間で両者の仕様を統合することが合意された。HA-APIはVersion2.0で凍結され、その後の活動はBioAPIの策定に注がれることになっている。こうして、新BioAPIは、BAPI、旧BioAPI、HA-APIの3つのAPIを統合した仕様として、1999年第4四半期末までにVersion1.0の完成を目指し(ドラフトは第3四半期末まで)、現在、作業が進行している(図3)。さらに、BioAPIコンソーシアムは外部の標準団体ともリエゾン関係を設け、Open GroupのCDSA/UAS (Common Data Security Architecture / User Authentication System)等、主要なコンピュータセキュリティの枠組にバイオメトリックスベースの認証サービスを付加する標準仕様の策定に対して影響力を持っている。

---

[1] http://www.senshubank.co.jp/teleban.html
[2] http://www.takefuji.co.jp/takefuji/html/721.html
[3] http://www.rhsecu.org/new.html
[4] http://www.nationwide.co.uk/whatsnew/whatsnewsetup.htm
[5] http://www.conavi.com/
(http://www.fingerscan.com.au/news/press_26-8-97.htm)
[6] http://www.bankofamerica.com/newsroom/press/press.cfm?PressID=press.19990106.01.htm
[7] http://www.mrpayroll.com/
(http://www.miros.com/MrPayroll_PR.htm)
[8] http://:www.saflink.com/haapi.html
[9] http://www.iosoftware.com/bapi/
[10] http://www.bioapi.org
[11] 他にも、特定のバイオメトリックス技術に依存しているものとしては、SRAPI(Speech Recognition API) Committeeが開発した、話者認識用APIのSVAPI (Speaker Verification API) などがある。

なお、日本では1999年5月セキュリティベンダー8社が「本人認証規格統一協議会」(PASO : Personal Authentication Standard Organization) を設立し、バイオメトリックス認証のAPIや共通評価基準策定のほか、米国のBioAPIに対し、日本の意見・要望を提出する活動を行っている。

一方、ISOなどの国際標準としては、個々にバイオメトリックス認証に関する提案が行われているのが実態である。ISO/IEC JTC1/SC17/WG4（接触端子つきICｶｰﾄﾞ）では、NWI (New Work Item)として接触式ICｶｰﾄﾞを使用したバイオメトリックス認証のAPI標準化の作業を行うことが決まっている。



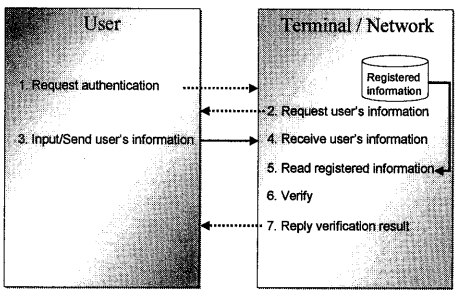
（図3）バイオメトリックスAPIの標準化の動向

5. バイオメトリックス認証の参照モデル

バイオメトリックス認証を実行するシステムの形態と必要とされる機能について考察する[12]。

(1) モデルI

本モデルにおける個人認証のプロセスは、例えば銀行キャッシュカードでATMより現金を引き出す場合に対応する。端末側あるいはセンターにユーザの個人性情報が予め登録されており、その情報に基づき本人の認証を行う。本モデルでは、ユーザは端末に直接アクセスすることを念頭においている。



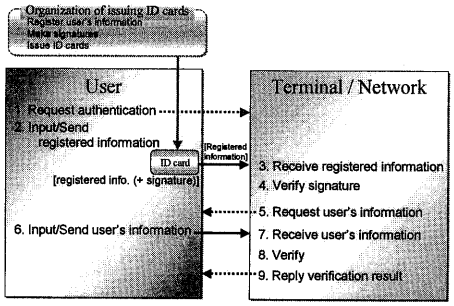
（図4）Authentication Model I

現在のキャッシュカードの安全性を高める目的で暗証番号＋バイオメトリックス認証を行う場合、従来の磁気カードをそのまま利用することも可能である。従来の暗証番号方式の脆弱性の問題をバイオメトリックス認証でカバーすることにより、カードの被害が減少することが期待される。

モデルIは、個人情報をシステム側で保管する点に特徴があるが、この情報が外部に露呈しないように、情報管理については万全の対策が必要とされる。また、システム側での個人情報の管理は、プライバシー保護の観点から利用を問題視するユーザも存在することを念頭に置く必要がある。

(2) モデルII

本モデルにおける個人認証のプロセスは、例えばクレジットカードによる本人の認証プロセスに対応している。個人情報を扱う場合、図5で示すIDカードはいわゆるICｶｰﾄﾞで実現される。



（図5）Authentication Model II

IDカードの発行機関は、ユーザの個人情報に署名を施してIDカードに記録・発行する。本モデルでは、ユーザはIDカードを端末に入力し、端末（もしくはネットワーク上のセンター機関）はIDカード内の情報を発行機関の署名とともに、入力された特徴パラメータとの類似性を確認することにより個人認証を実行する。

本モデルの特徴は、個人情報を各個人が自ら管理できる点にある。IDカードの発行機関がカード発行後に原個人情報を破棄すれば、プライバシーの問題はモデルIと比較して大幅に軽減できる。このため、モデルIIではバイオメトリックス認証を普及させる上で、主要な課題の一つである社会的なコンセンサスを得ることができる可能性がある。また、バンキングシステムにおいても、ICｶｰﾄﾞの適用に伴うカード内情報の機密性を確保するうえでも、本モデルによるバイオメトリックス認証の適用は有効と考えられる。

当面IDカードの発行機関は各銀行とするのが現実的であるが、一銀行機関に止まらずバンキングシステム全体で適用するためには、いわゆる認証局と同様の機関によって発行されることも考えられる。さらにこの認証局の実現により、個人認証が必要とされる多くのシステムに本モデルが共通に適用可能となる。

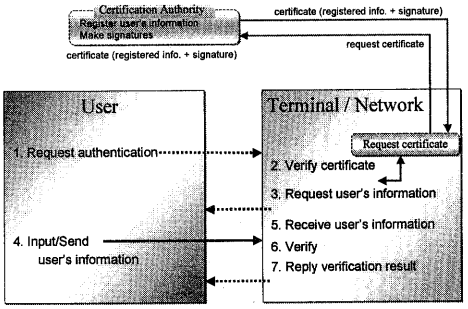
本モデルでは、IDカードの物理的な安全性はもちろ

[12]システムモデルについては、本人認証技術検討WG中間報告書（1997年5月 電子商取引実証推進協議会）を参考にした。

んのこと、端末内から不正な手段で個人情報がコピーされないような対策（耐タンパー性）が必要となる。

(3) モデルⅢ

モデルⅢでは、ユーザはネットワークを介してセンターにアクセスすることを念頭に置いており、個人情報は全て認証機関が管理する点に特徴がある。この認証機関は、いわゆる公開鍵を提供する一般の認証局の機能を拡大した機関と位置づけられる。



（図6）Authentication Model III

センターは、ユーザからの認証要求があると、認証機関に証明書を要求する。この証明書には、ユーザの個人情報と認証機関の署名が含まれている。証明書を入手した後の認証プロセスは、モデルⅠもしくはモデルⅡと同様である。

本モデルは、バンキングシステムに係わらず、多くの個人認証を必要とするシステムに適用可能である。センターは、認証機関に証明書を要求する際にユーザの revocation list を参照することも可能となる[13]。

個人認証の目的のためには、ユーザは何も所持する必要がない究極の形態とも考えられるが、ネットワーク上を個人情報が流れることに対するセキュリティ対策、またモデルⅠおよびⅡと同様に端末内での個人情報の不正な入手対策を講じる必要がある。

来るべき高齢化社会においては、モデルⅢに示す認証システムの必要も高まることが考えられる。このためにも、モデルⅠあるいはモデルⅡのシステムでバイオメトリックス認証の社会的認知を得ておくことは必要である。

モデルⅠ～Ⅲにおいて、当面バイオメトリックス認証は現状の暗証番号方式に対する補足的な手段として用いられることになろう。ここで、バイオメトリックス認証に対して極めて強力な安全性を要求する必要は必ずしもない。例えばモデルⅠあるいはモデルⅡにおいては、ユーザがカードを紛失して、センターがカードを無効とするまでの機関における安全性が現状よりも向上する程度で十分な効果はあり、安全レベルを幾つか設定して、それをユーザが自ら選択する形態も考えられる。ここで重要なことは、カード、端末等の小型化、低廉化を十分念頭に置き、バイオメトリックス認証の社会的コンセンサスを得る原動力となる実用化を考慮することであろう。

6. バイオメトリックス認証の課題

バイオメトリックス認証における主要な課題としては、第1に社会的な容認、コンセンサスづくりの必要性、第2に操作の容易性、第3に当然のことながら安全性の高さ、第4にコストの低廉化が挙げられる。特に個人のプライバシーに関わる情報を扱うため、こうした社会的な配慮を施すことによってコンセンサスを得ることは不可欠となる。誰もしくはどの機関がバイオメトリックス情報を登録して管理するのかという運用面、法規面の問題も、これに関連して重要である。

さらに、ネットワークを介して広くバイオメトリックス技術を利用していくためには、4 章で述べた API を浸透させ、適用するバイオメトリックス技術変更の容易性と複数のアプリケーションに対する拡張、さらには複数のバイオメトリックス技術の利用を実現する必要がある。

1992 年英国において、APACS で最小限のバイオメトリックス認証に対する基準が策定されている[3]。これによると、タイプⅠエラー：0.001%、タイプⅡエラー：5.00%、認証時間：3 秒、価格：150 ポンド以下、デザイン：単体もしくは組み込み、となっている。現状の技術で、バイオメトリックス認証全てについて上記の基準を満足することは困難と考えられるが、複数のパラメータの組み合せにより実現できる可能性はあろう。また、こうした基準自体についても、利用環境、財産規模等を考慮した複数のレベルを検討する必要がある。

いずれにせよ、バイオメトリックス認証は、ローカルで利用されている技術が改良を重ねながら広く世の中に浸透してくものと思われる。こうしたバイオメトリックス技術の利用は、携帯あるいは記憶する必要が無いなど高齢者にとっても利便性の高い個人認証方式であり、高齢化社会を目前に控えた我が国でも有用な技術として期待できる。

【参考文献】

[1] 小松尚久, "個人認証の技術動向", 画像電子学会誌, 第 27 巻第 3 号, pp.196-204, 1998.

[2] 安田浩, "Things Thinking —全てが情報発信—", 画像電子学会第 27 回年次大会予稿集, p.63, 1999.6

[3] "Biometrics: A Snapshot of Current Activity – 1996", European Committee for Banking Standards

[13] モデルⅡでは、端末もしくはセンター機関からカード発行機関へのアクセスについては特に示していないが、revocation list の参照を行う際には必要である。